Available at: http://www.ictp.trieste.it/~pub_off IC/2001/132

United Nations Educational Scientific and Cultural Organization
and
International Atomic Energy Agency
THE ABDUS SALAM INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

SUBGROUPS OF CLASS GROUPS OF ALGEBRAIC QUADRATIC FUNCTION FIELDS

Kunpeng Wang
Graduate School, Academia Sinica,
Beijing 100039, People's Republic of China

and

Xianke Zhang[1]
Tsinghua University, Department of Mathematics,
Beijing 100084, People's Republic of China
and
The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

Ideal class groups $H(K)$ of algebraic quadratic function fields K are studied, by using mainly the theory of continued fractions of algebraic functions. Properties of such continued fractions are discussed first. Then a necessary and sufficient condition is given for the class group $H(K)$ to contain a cyclic subgroup of any order n, this criterion condition holds true for both real and imaginary fields K. Furthermore, several series of function fields K, including real, inertia imaginary, as well as ramified imaginary quadratic function fields, are given, and their class groups $H(K)$ are proved to contain cyclic subgroups of order n.

MIRAMARE – TRIESTE
September 2001

[1] Regular Associate of the Abdus Salam ICTP.

I. Introduction and Statement of Main Results

Let $k = \mathbf{F}_q(T)$ be the rational function field of the indeterminate T over the field $\mathbf{F}_q$, where $\mathbf{F}_q$ is the finite field with q elements, q a power of any odd prime number. Let $R = \mathbf{F}_q[T]$ be the ring of polynomial forms of T over $\mathbf{F}_q$. Any finite extension K of k is said to be an algebraic function field. The integral closure of R in K is denoted by $\mathcal{O}_K$, which is a Dedekind domain. The ideal class group of $\mathcal{O}_K$ is denoted by $H(K)$ and is called the ideal class group of K. $h(K) = \#H(K)$ is called the ideal class number of K.

A quadratic extension of k could be written as $K = k(\sqrt{D})$, where D is a square-free polynomial in R. When deg$D$ (the degree of D) is even and D is monic, $K = k(\sqrt{D})$ is said to be real; when deg$D$ is even and the coefficient of its highest term is not a square (we may then assume it is g, the generator of the multiplicative group $\mathbf{F}_q^\times$), $K = k(\sqrt{D})$ is said to be inertia imaginary; and when deg$D$ is odd, $K = k(\sqrt{D})$ is said to be ramified imaginary. Also D is said to be positive (or negative) when $K = k(\sqrt{D})$ is real (or imaginary respectively). These terms come from different behaviors of decompositions in K of the infinity prime divisor (valuation) ∞ of k.

We are interested in the ideal class group $H(K) = H(D)$ and the ideal class number $h(K) = h(D)$ of a quadratic function field $K = k(\sqrt{D})$. Friesen in [1] studied real quadratic function field

$$K = k(\sqrt{G^{2n} + c^2})$$

(with $G \in R,\ c \in \mathbf{F}_q^\times$), and proved that $h(K)$ is divisible by n (written $n|h(K)$). This result was generalized to $n|h(K)$ for any quadratic field

$$K = k(\sqrt{G^{2n} + H})$$

(with $G, H \in R,\ H|G$) in[2]. We also gave a quite systematical discussion on quadratic function fields and the continued fraction theory of functions in [3]. Ichimura in [4] studied imaginary quadratic fields

$$K = k(\sqrt{T^{\ell^n} + c}),$$

($T \in R,\ c \in \mathbf{F}_q^\times,\ \ell$ is an odd prime number and $(\ell,\ q) = 1$), giving conditions for $\ell|h(K)$. A corollary in the present paper will show that for fields K in [4] we actually have $\ell^n|h(K)$ rather than $\ell|h(K)$ under most conditions. Here we will also give a criterion for the class group $H(K)$ to contain a cyclic subgroup of any order n, which is valid for both real and imaginary fields K. Furthermore, we will provide several series of function fields K with $H(K)$ containing cyclic subgroups of order n.

In [5], a necessary and sufficient condition is given for a real quadratic number field $F = \mathbf{Q}(\sqrt{d})$ to have an ideal class group containing a cyclic subgroup of order n; and, by using

this condition and theory of continued fractions, several series of real quadratic number fields with class groups containing subgroups of order n are constructed. Here we will obtain results about $H(K)$ containing a cyclic subgroup of order n for general quadratic function fields K (i.e., for real, inertia imaginary, and ramified imaginary quadratic function fields K), by using semi-simple continued fractions of functions.

The following Theorem 1 is valid for both real and imaginary fields K. And a proper solution is a solution $X, Y \in R$ with $(X,\ Y) = 1$.

Theorem 1. Let $K = k(\sqrt{D})$ be a quadratic function field, real or imaginry. The ideal class group $H(K) = H(D)$ contains a cyclic subgroup of order n if and only if the equation

$$X^2 - DY^2 = cZ^n$$

has a proper solution (X, Y) (for some $c \in \mathbf{F}_q^{\times}$ and $Z \in R - \mathbf{F}_q$), and the equation

$$X^2 - DY^2 = bZ^m$$

has no proper solution (for any $b \in \mathbf{F}_q^{\times},\ 1 \leq m | n,\ m < n$).

Theorem 2. Let $D = B^2 + M^n,\ \deg B^2 < \deg M^n,$ where B and M are polynomials in R, $\deg M$ is odd, $\gcd(M, B) = 1$, n is odd. Then $K = k(\sqrt{D})$ is an inertia imaginary quadratic function field, and its ideal class group $H(D)$ contains a cyclic subgroup of order n.

Corollary 1. Let $D = M^n + c^2$ where $\deg M$ and n are odd (i.e. take $B = c \in \mathbf{F}_q^{\times}$ in Theorem 2), then $H(D)$ contains a cyclic subgroup of order n, and $n | h(D)$.

Theorem 3. Let $D = B^2 + gM^{2n},\ \deg B < \deg M^n,$ where B and M are polynomials in R, M is monic with even degree, $\gcd(B, M) = 1$, g is a generator of the multiplicative group $\mathbf{F}_q^{\times}$; n any positive integer. Then $K = k(\sqrt{D})$ is an inertia imaginary quadratic function field, and its ideal class group $H(D)$ contains a cyclic subgroup of order $2n$, inparticularly, $2n | h(D)$.

Corollary 2. Let $D = gM^{2n} + c^2$ where M is monic with even degree (i.e. take $B = c \in \mathbf{F}_q^{\times}$ in Theorem 3). Then the ideal class $H(D)$ of $K = k(\sqrt{D})$ contains a cyclic subgroup of order $2n$, and $2n | h(D)$.

Theorem 4. For the following square-free polynomial

$$D = ((eZ^n + N)/2U - U)^2 + 2N,$$

the ideal class group $H(D)$ of the real quadratic function field $K = k(\sqrt{D})$ has a cyclic subgroup of order n, where $e \in \mathbf{F}_q^{\times}$, Z, N, U are polynomials in $R - \mathbf{F}_q^{\times}$ satisfying $N \not| Z^n$, $\deg N \geq \frac{1}{2} \deg Z^n$, $U | (eZ^n + N)$, $VH + 1 = 2rN$, and $2(eZ^n + N)/2U - U) = 2NV + H$ for some $V, H \in R$ with $0 \leq \deg H < \deg N,\ \deg V > 0,\ r \in \mathbf{F}_q^{\times},$ and $n \geq 2$.

Example for theorem 4. In theorem 4, let $k = \mathbf{F}_3(T)$, $e = 2$, $Z = T^2 + 1$, $N = 2T^3 + T + 2$, $U = T^2 + 2, n = 3$. Then

$$D = T^8 + 2T^5 + T^4 + T^3 + T^2 + 2.$$

So the ideal class group $H(D)$ of $K = k(\sqrt{D})$ has a cyclic subgroup of degree 3, and $3|h(D)$. In fact, it has been proved that $h(D) = 3$ (cf [6]).

II. Semi-simple Continued Fractions of Functions and Quadratic Diophantine Equations

We now give a brief introduction to (semi-simple) continued fractions of functions and some properties of them (see [7] for details). An expression of the form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots}} \quad , \qquad (b_i \in R = \mathbf{F}_q[T])$$

is said to be a (semi-simple) continued fraction of functions, which is usually written as $\alpha = [b_0, b_1, \cdots]$. Also $p_n/q_n = [b_0, b_1, \cdots, b_n]$ is called the $n-$th convergent of α, and $\alpha_n = [b_n, b_{n+1}, \cdots]$ is called the n-th complete quotient of α. (The above continued fractions are said to be "semi-simple" since the concerned b_i are not restricted to be " positive" (as defined at the beginning of section I), which correspond to the semi-simple continued fractions of numbers.)

Continued fractions $\alpha = [b_0, b_1, \cdots]$ of functions above have the following properties. Most of them are similar to those of continued fractions of numbers (In fact, they are deduced formaly from the special form of continued fractions, so the proofs will be ommitted). Nevertheless, continued fractions of functions also have special properties of their own.

Proposition 2.1.

(I) $p_0 = b_0,\ p_1 = b_0b_1 + 1,\ p_n = b_np_{n-1} + p_{n-2} \quad (n \geq 2);$
$q_0 = 1, \quad q_1 = b_1, \qquad q_n = b_nq_{n-1} + q_{n-2} \quad (n \geq 2).$

(II) $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1} \quad (n \geq 1);$
$p_nq_{n-2} - p_{n-2}q_n = (-1)^n b_n \quad (n \geq 2).$

(III)
$$\alpha = \frac{p_{n-1}\alpha_n - p_{n-2}}{q_{n-1}\alpha_n - q_{n-2}}.$$

Proposition 2.2. If $\deg b_i > 0 \quad (0 \leq i \leq n)$, then

$$\deg(p_n/q_n) = \deg(p_{n-1}/q_{n-1});$$

$$\deg p_n = \sum_{i=0}^{n} \deg b_i \geq n;$$

$$\deg q_n = \sum_{i=1}^{n} \deg b_i \geq n.$$

For a squarefree polynomial $D \in R = \mathbf{F}_q[T]$, the square root $\sqrt{D}$ could be expanded into a (semi-simple) continued fraction via the following procedure (**CONT**):

CONT 1. Take any $b_0 \in R$, then $\alpha_0 = \sqrt{D} = b_0 + \sqrt{D} - b_0$. Put

$$\alpha_1 = \frac{1}{\sqrt{D} - b_0} = \frac{\sqrt{D} + b_0}{D - b_0^2} = \frac{\sqrt{D} + P_1}{Q_1},$$

where we have let $P_1 = b_0$, $Q_1 = D - b_0^2$.

CONT 2. Take any $b_1 \in R$, then $\alpha_1 = b_1 + (\sqrt{D} - (b_1 Q_1 - P_1))/Q_1$. Put

$$\alpha_2 = \frac{Q_1}{\sqrt{D} - (b_1 Q_1 - P_1)} = \frac{\sqrt{D} + (b_1 Q_1 - P_1)}{(D - (b_1 Q_1 - P_1)^2)/Q_1} = \frac{\sqrt{D} + P_2}{Q_2},$$

where we have put $P_2 = b_1 Q_1 - P_1$, $Q_2 = (D - (b_1 Q_1 - P_1)^2)/Q_1$. It's easy to see $P_2,\ Q_2 \in R$.

Continuing the above procedure we expand $\sqrt{D}$ into a semi-simple continued fraction

$$\sqrt{D} = [b_0, b_1, \cdots, b_{n-1}, \alpha_n],$$

and obtain

$$\alpha_n = \frac{\sqrt{D} + P_n}{Q_n} \qquad\qquad (n > 1)$$

with P_n, $Q_n \in R$. Q_n is called the n-th complete denominator. Also note that we obviously have the following relation for its $(n-1)-$th convergent p_{n-1}/q_{n-1} and $n-$th complete denominator Q_n similar to that for continued fractions of numbers:

$$p_{n-1}^2 - q_{n-1}^2 D = (-1)^n Q_n.$$

Remark 1. If D is "positive" (i.e., monic with $\deg D = 2d$ even), then in the above procedure we could take b_n in a certain way and obtain"the **simple** continued fraction" for $\sqrt{D}$. In fact, a "positive" D could be written as $D = \Delta^2 + r$ uniquely (with $\deg\Delta = d, \deg r < d$, $\Delta, r \in R$, Δ monic), then we take b_n as the "quotient" of $\Delta + P_n$ divided by Q_n: i.e., $\Delta + P_n = b_n Q_n + r_n$ with $\deg r_n < \deg Q_n$. (see [6])

We now use semi-simple continued fractions of functions to discuss Diophantine equations of functions:

$$X^2 - DY^2 = C \qquad\qquad (D, C \in R = \mathbf{F}_q[T]). \tag{1}$$

A solution $(X, Y) \in R^2$ of (1) is denoted also by $\theta = X + Y\sqrt{D}$. Its conjugate $\bar{\theta} = X - Y\sqrt{D}$ and associate $\varepsilon\theta$ of θ are also solutions of (1), where $\varepsilon = U + V\sqrt{D}$ satisfies $\mathrm{N}(\varepsilon) = U^2 - V^2 D \in \mathbf{F}_q^{\times}$, $\quad U, V \in R$.

Now define $A_i = A_i(U_1, \cdots, U_i)$, $B_i = B_i(U_1, \cdots, U_i) \in R[U_1, \cdots, U_i]$ as polynomials of $U_1, \cdots, U_i$ by induction as the following:

$$\begin{cases} A_i = U_i A_{i-1} + A_{i-2}, & A_0 = 1, \quad A_1 = U_1, \\ B_i = U_i B_{i-1} + B_{i-2}, & B_0 = 0, \quad B_1 = 1, \end{cases}$$

where $U_1, \cdots, U_i$ are distinct indeterminates (and will be assumed to be polynomials in R). For any expression $D = F^2 + G$ with $F,\ G \in R = \mathbf{F}_q[T]$, define

$$\begin{array}{ll} \theta_i^* = A_i + B_i\sqrt{D}, & C_i^* = A_i^2 - B_i^2 D, \\ \theta_i = (FB_i + A_i) + B_i\sqrt{D}, & C_i = 2FA_iB_i - B_i^2 G + A_i^2. \\ T_i(1) = \{\theta_i | U_1, \cdots, U_i \in R\}, & C_i(1) = \{C_i | U_1, \cdots, U_i \in R\}. \end{array}$$

Proposition 2.3. Equation (1) has a proper solution if and only if one of the following holds:

(a) $C = C_i^*$ for some $0 \le i \in \mathbf{Z}$ and some $U_1, U_2, \cdots, U_i \in R$. And if so, all the solutions are just θ_i^* together with its associates and conjugates.

(b) $C = C_i$ for some $0 \le i \in \mathbf{Z}$ and some $U_1, U_2, \cdots, U_i \in R$. And if so, all the solutions are just θ_i together with its associates and conjugates.

(c) $C \in C_i(1)$ for some $0 \le i \in \mathbf{Z}$. And if so, all the solutions are just $T_i(1)$.

Proof. (a) First, assume that $X^2 - DY^2 = C$ has a proper solution (X, Y). Using the division algorithm we obtain the simple continued fraction expansion $X/Y = [U_1, \cdots, U_i]$, which is finite with $U_1, \cdots, U_i \in R$. Thus we can obtain an "$i-$step" expansion of $\sqrt{D}$ as a semi-simple continued fraction:

$$\sqrt{D} = [U_1, U_2, \cdots, U_i, \alpha_i].$$

For this continued fraction we have $p_{i-1}/q_{i-1} = [U_1, U_2 \cdots, U_i] = X/Y$, $\alpha_i = (\sqrt{D} + P_i)/Q_i$, and $p_{i-1}^2 - q_{i-1}^2 D = (-1)^i Q_i$. So we have $p_{i-1} = X$, $q_{i-1} = Y$ since $(X,\ Y) = (p_{i-1},\ q_{i-1}) = 1$. Thus

$$C = X^2 - DY^2 = p_{i-1}^2 - Dq_{i-1}^2 = (-1)^i Q_i.$$

By the definition of $A_i(U_1, \cdots, U_i)$ and $B_i(U_1, \cdots, U_i)$ we know

$$X = p_{i-1} = A_i(U_1, \cdots, U_i), \quad Y = q_{i-1} = B_i(U_1, \cdots, U_i),$$

$$X + Y\sqrt{D} = A_i + B_i\sqrt{D} = \theta_i^*.$$

$$C = X^2 - DY^2 = \mathrm{N}(A_i + B_i\sqrt{D}) = C_i^* = \mathrm{N}(\theta_i^*).$$

On the other hand, if $C = C_i^* = A_i^2 - B_i^2 D$ for some $0 \le i \in \mathbf{Z}$ and some $U_1, U_2, \cdots, U_i \in R$. Then we can construct a semi-simple continued fraction of $i-$step for $\sqrt{D}$:

$$\sqrt{D} = [U_1, \cdots, U_i, \alpha_i].$$

So for this continued fraction we have $p_{i-1} = A_i(U_1, U_2, \cdots, U_i), q_{i-1} = B_i(U_1, U_2, \cdots, U_i)$ by definition of A_i and B_i, thus $(-1)^i Q_i = p_{i-1}^2 - q_{i-1}^2 D = A_i^2 - B_i^2 D = C_i^* = C$. Hence the equation $X^2 - DY^2 = C$ has a proper solution $\theta_i^* = A_i + B_i\sqrt{D}$.

(b) Let us discuss first the relation of $\theta_i^*,\ C_i^*$ and $\theta_i,\ C_i$. By the definitions of $A_i,\ B_i$ we may prove the following via induction:

$$A_i = \begin{vmatrix} U_1 & -1 & & \\ 1 & \ddots & \ddots & \\ & \ddots & \ddots & -1 \\ & & 1 & U_i \end{vmatrix}, \quad B_i = \begin{vmatrix} U_2 & -1 & & \\ 1 & \ddots & \ddots & \\ & \ddots & \ddots & -1 \\ & & 1 & U_i \end{vmatrix}.$$

$$FB_i + A_i = \begin{vmatrix} F+U_1 & -1 & & & \\ 1 & U_2 & -1 & & \\ & 1 & \ddots & \ddots & \\ & & \ddots & \ddots & -1 \\ & & & 1 & U_i \end{vmatrix}$$

$$= A_i(F + U_1, U_2, \cdots, U_i)$$

$$= \tilde{A}_i(U_1, U_2, \cdots, U_i) = \tilde{A}_i.$$

Thus we have

$$\theta_i = (FB_i + A_i) + B_i\sqrt{D} = \tilde{A}_i + B_i\sqrt{D} = A_i(F + U_1, U_2, \cdots, U_i) + B_i\sqrt{D}$$

$$= \theta_i^*(F + U_1, U_2, \cdots, U_i),$$

$$C_i = \tilde{A}_i^{\,2} - B_i^2 D = C_i^*(F + U_1, U_2, \cdots, U_i).$$

This proves (b) since U_i are arbitrary.

(c) By definition of $T_i(1)$ and $C_i(1)$, this is obvious. □

Remark 2. The above theory about semi-simple continued fraction and Diophantine equations is also valid for numbers (and even imaginary numbers). For example, we have the following expansion of semi-simple continued fraction of $\sqrt{-1}$:

$$\sqrt{-1} = [1, 1, 1, 1, 1, \cdots].$$

Its denominators are

$$\{Q_i\}_{i=0,1,\cdots} = \{1, -2, 5, -13, 34, -89, \cdots\}.$$

So all the corresponding $(-1)^i Q_i$ $(i \geq 1)$ $(=1,\ 2,\ 5,\ 13,\ 34,\ 89\cdots)$ are sums of two integer squares, *e.g.*, $89 = 8^2 + 5^2$. In fact, in this way we could obtain all those integers which are sums of two integer squares. This point will be discussed in another paper.

III Proofs of the Main Results

Proof of Theorem 1. Assume the equation $X^2 - Y^2 D = cZ^n$ has a proper solution $X = A$, $Y = B$ in R. Put $\theta = A + B\sqrt{D}$, then

$$\theta\overline{\theta} = A^2 - B^2 D = cZ^n,$$

where $\overline{\theta} = A - B\sqrt{D}$ is the conjugate of θ. Suppose that $Z = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m}$ is the factorization of Z(P_i are distinct irreducible polynomials in R, $e_i \geq 1$ ($i = 1, 2, \cdots, m$)). Then for any irreducible factor P of Z we have $B^2 D \equiv A^2 \pmod{P}$. Since D is squarefree, $(A, B) = 1$, and $n \geq 2$, it is easy to show that $P \not| A$, $P \not| B$, $P \not| D$. For example, if $P|A$, the $P \not| B$, $P|D$; so $P||D$; from $A^2 - B^2 D \equiv cZ^n \pmod{P^2}$, we get $0 - B^2 D \equiv 0 \pmod{P^2}$, a contradiction. Thus the Legendre symbol

$$\left(\frac{D}{P}\right) = \left(\frac{B^2 D}{P}\right) = \left(\frac{A^2}{P}\right) = 1.$$

So P is completely splitting in K . Assume the factorization of $P_i|Z$ is as follows:

$$(P_i) = \wp_i \overline{\wp}_i \quad (i = 1, 2, \cdots, m).$$

So we have the ideal equation $\theta\overline{\theta} = (Z^n) = (P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m})^n = (\wp_1^{e_1} \overline{\wp}_1^{e_1} \wp_2^{e_2} \overline{\wp}_2^{e_2} \cdots \wp_m^{e_m} \overline{\wp}_m^{e_m})^n$. Note that θ has not factor in R, and θ is relatively prime to $\overline{\theta}$ (In fact, if $P|(\theta, \overline{\theta})$, then $P|(\theta + \overline{\theta}$, $\theta - \overline{\theta}) = (A,\ BD) = (A,\ D)$, so $P|\theta$ and $P|D$, which contradicts to the fact that the factors of θ are splitting, while factors of D are ramified). So we may assume

$$(\theta) = I^n,$$

where $I = \hat{\wp}_1^{e_1} \hat{\wp}_2^{e_2} \cdots \hat{\wp}_m^{e_m}$ ($\hat{\wp}_i = \wp_i$ or $\overline{\wp}_i$, $\quad i = 1, 2, \cdots, m$). Thus I^n is a principal ideal. If $j|n$ and I^j is principal, we would put

$$I^j = (\alpha),$$

where $\alpha = X_1 + Y_1\sqrt{D} \in \mathcal{O}_K$ $(X_1, Y_1 \in R)$. Then

$$(Z^j) = I^j \overline{I^j} = (\alpha\overline{\alpha}) = (X_1^2 - DY_1^2),$$

that is

$$X_1^2 - DY_1^2 = c' Z^j$$

($c' \in \mathbf{F}_q$). Since we have assumed $X^2 - DY^2 = c' Z^j \quad (1 \leq j|n, j \neq n)$ has no proper solution in the Theorem, so I^j is not principal. Therefore, I generates a cyclic subgroup of order n in $H(D)$.

On the other hand, if $H(D)$ contains a cyclic subgroup of order n, we may assume it is generated by $[I]$, the class represented by an integral ideal I . Then I^n is a principal ideal, and we may assume I is completely splitting. Then

$$I^n = (\theta), \quad \theta = A + B\sqrt{D} \in \mathcal{O}_K.$$

So

$$(A^2 - B^2 D) = (\theta\overline{\theta}) = (I\overline{I})^n = (Z^n).$$

That is

$$A^2 - B^2 D = cZ^n, (c \in \mathbf{F}_q^\times),$$

where Z is the norm of I. On the other hand, we know $X^2 - DY^2 = c'Z^j \quad (1 \leq j | n, j \neq n)$ has no proper solution (otherwise, $[I]$ would generate a subgroup in $H(D)$ with order $\leq j < n$, a contradiction). This proves the Theorem 1. □

Proof of Theorem 2. Obviously $(X, Y) = (B, 1)$ is a proper solution of the equation $X^2 - DY^2 = -M^n$. By Theorem 1 we know it is sufficient to prove $X^2 - DY^2 = cM^m$ has no solution (for $1 \leq m | n,\ m \neq n,\ c \in \mathbf{F}_q^\times$). It follows from the facts that the degree of $X^2 - DY^2$ is bigger or equal to degree of D (note deg$D$ is odd) for any $X, Y \in R$, and $\deg B^2 < \deg M^n$, $D = B^2 + M^n$. So deg$D$ cannot be less than degM^n as the equation $X^2 - DY^2 = cM^m$ needs. □

Proof of Theorem 3. Note that $(X, Y) = (B, 1)$ is a solution of the equation $X^2 - DY^2 = -gM^{2n}$. So by Theorem 1 we need only to prove that $X^2 - DY^2 = cM^m$ has no solution (for $1 \leq m | 2n,\ m \neq 2n,\ c \in \mathbf{F}_q^\times$). In fact, the degree of $X^2 - DY^2$ cannot be less than the degree of D for any $X, Y \in R$, (note that D has even degree and its coefficient of highest term is not a square, while X^2, Y^2 has squares being their coefficients of highest terms, so X^2 and DY^2 have different highest terms as polynomials of T), and the degree of $D = B^2 - gM^{2n}$ ($\deg B^2 < \deg M^{2n}$) is $2n \deg M$, which is bigger than degM^m $= m \deg M$ (since $2n > m$). Thus the degree of $X^2 - DY^2$ is bigger than the degree of M^m, so $X^2 - DY^2 = cM^m$ has no solution. □

Proof of Theorem 4. Note that $B = (eZ^n + N)/2U - U \in R$ since $U | (eZ^n + N)$. Thus the equation $X^2 - DY^2 = cZ^n$ has a solution in R since

$$(B + 2U)^2 - D = 2eZ^n.$$

So by theorem 1, we need only to show that the equation $X^2 - DY^2 = cZ^{n'}$ has no solution in R for $1 \leq n' | n,\ n' \neq n,\ c \in \mathbf{F}_q^\times$.

Note that by the conditions in the theorem we have $2B = 2NV + H$ with $\deg B > \deg N$ (since $\deg V > 0$) and deg$H$ <deg$N$. Thus $\deg N < \deg Z^n$ since $B = (eZ^n + N)/2U - U \in R$.

Using the fact $D = B^2 + 2N$, $2B = 2NV + H$, $VH + 1 = 2rN$ and the degree conditions, we obtain the expansion of **simple** continued fraction for $\sqrt{D}$:

$$\sqrt{D} = [B,\ \overline{V,\ V,\ 2B}] \qquad (\text{if } r = 1);$$

$$\sqrt{D} = [B,\ \overline{V,\ r^{-1}V,\ 2rB,\ r^{-1}V,\ V,\ 2B}] \qquad (\text{if } r \neq 1).$$

and obtain all the denominators $\{Q_i\}$ of complete quotients of this expansion in both cases :

$$\{1,\ 2N\} \qquad (\text{if} r = 1);$$

$$\{1,\ 2N,\ 2rN,\ r^{-1}\} \quad (\text{if } r \neq 1).$$

Note that in both cases it is impossible that $cZ^{n'} = 2N$ or $2rN$ (for $n'|n,\ n' \neq n$), since $\deg N \geq \frac{1}{2}\deg Z^n,\ N \not| Z^n$.

In [3] we have proved that the equation $X^2 - DY^2 = C$ (with $\deg C < \frac{1}{2}\deg D$) has a proper solution if and only if C is a denominator (up to a constant) of complete quotient in the expansion of simple continued fraction of $\sqrt{D}$. For our equation $X^2 - DY^2 = cZ^{n'}$, we know $\deg(cZ^{n'}) < \frac{1}{2}\deg D$; in fact by $\deg B > \deg N$ we know $\deg D = \deg(B^2 + 2N) = \deg B^2$, thus $\deg Z^{n'} \leq \frac{1}{2}\deg Z^n \leq \deg N < \deg B = \frac{1}{2}\deg D$. Therefore, the above argument about $cZ^{n'} \neq 2N$ or $2rN$ means that the equation $X^2 - DY^2 = cZ^{n'}$ has no solution in R for $1 \leq n'|n,\ n' \neq n,\ c \in \mathbf{F}_q^{\times}$. By Theorem 1, we know that the ideal class group $H(D)$ of $K = k(\sqrt{D})$ has a cyclic subgroup of degree n, and $n|h(D)$.

Acknowledgments. X.Z. was supported by the National Natural Foundation of China. This work was done within the framework of the Associateship Scheme of the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

References

[1] Friesen C., Class Number Divisibility in Real Quadratic Function Fields, Canad. Math. Bull. **35**(1992)361–370

[2] ZHANG Xianke & WANG Kunpeng, Ideal classgroups and subgroups of real quadratic function fields, Tsinghua Science and Technology, 5(2000), No.4: 372-373

[3] Wang Kunpeng, Arithmetic Structure of Quadratic Function Fields, Dissertation, Tsinghua University, Beijing, 2000.

[4] Ichimura H., Quadratic Function Fields Whose Class Numbers are Not Divisible by Three,Acta Arithmetica. **XCI**(1999)181–190

[5] ZHANG Xianke and Washington L. C. , Ideal Class Groups and Their Subgroups of Real Quadratic Fields, Science in China, **27** (1997) 523–528

[6] Feng, K. & Sun, S., On Class Number of Quadratic Function Fields, Proceeding of First International Symposium on Algebraic Structures and Number Theory(1988, Hong Kong),Lam, S.P. & Shum, K.P. Edts., World Scientific, 1990, 88–133

[7] WANG Kunpeng & ZHANG Xianke , The continued fractions connected with quadratic function fields, Advanced in Math. 29(2000. 8), No.4, 375-377.